



July 2012

Revision 1.2

© 2015 ZIH Corp. All rights reserved. Zebra and the Stylized Zebra Head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. All other trademarks are property of their respective owners.

Table of Contents

Table of Contents.....	3
1. Overview.....	4
1.1 Limitations	4
1.2 Web User Interface	5
1.3 Components	7
2. Configuration	7
2.1 Configuration Details.....	7
2.1.1 Licensing	7
2.1.2 Firewall – Protocols.....	8
2.1.3 RADIUS and AAA Policies	9
2.1.4 Captive Portal Policies	11
2.1.5 Wireless LAN	13
2.1.6 HTTP Analysis	14
3. Nearbuy Systems Solution	15
3.1 Nearbuy External Server Configuration.....	15
3.2 HTTP Analysis	16
4. Appendix.....	17
4.1 Running Configuration	17

1. Overview

An important and much anticipated feature in WiNG 5.4 is that of HotSpot Analytics. This licensed module provides details and history on a user's web browsing behavior and on the different device and operating system types on a captive portal enabled wireless LAN and provides a wealth of information to businesses to understand the web browsing habits of their customers, as related to their business. This has obvious value in the retail space.

Additionally, WiNG 5.4 will introduce guest on-boarding, in conjunction with a guest-access captive portal WLAN. This allows a WiNG 5.4 and later device to dynamically learn the MAC addresses of guest clients and store them so that subsequent associations are not redirected to the captive portal splash page.

The analytics module does require a license, though it does not require licensing on both controllers within a cluster; the second controller in the cluster will have knowledge of the analytics database that is built over time. Additionally, analytics is only available on the NX9 series of controllers (NX9000 / NX9500).

1.1 Limitations

As stated previously, the Analytics function is only available on the NX9xxx platform. If a Nearbuy Systems solution has been sold to the customer, It is also needed in addition to Nearbuy Systems; in this case we are forwarding guest wifi web traffic to an external / centralized analytics engine (Nearbuy Systems).

Because some browsers and devices will allow some configuration of the user agent string, it is not always possible to know exactly what type of device is making the call. Thus, the data in the graphs may not always state all client-type devices which are in use. As an example, an Android mobile client browser that allows the user to enable a desktop user-agent, so that the user can view the full, standard website as opposed to the mobile website.

Finally, because of the predictive nature of modern search engines, one may often see URL's or search terms that have not actually been sought by the user. One common example is to see www.google-analytics.com as a top URL, as this is happening in the background, respective to the user.

1.2 Web User Interface

The analytics graphs are found under Statics / Analytics on your controller. By default, history for the entire System is shown; you can drill down to a location level by click on the desired RF-Domain in the left pane:

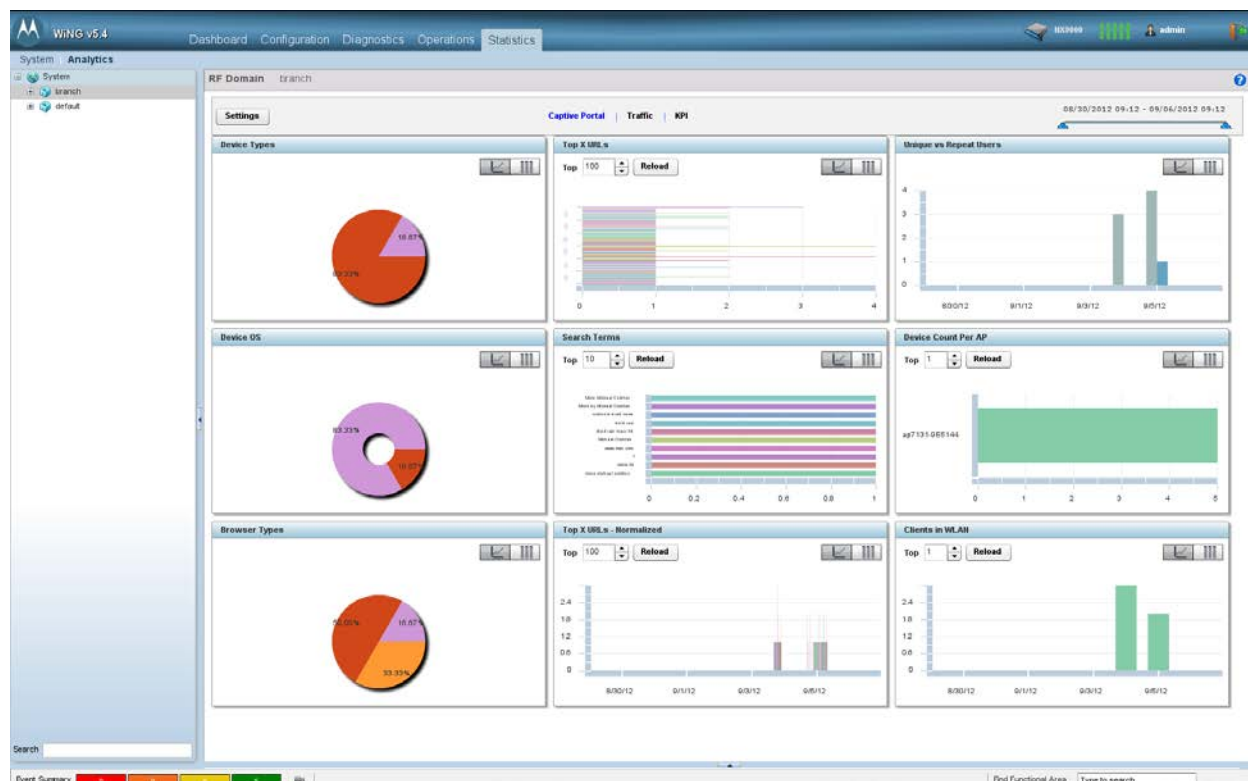


Figure 1 - Analytics Dashboard

The **Settings** button will allow an administrator to specify the time period for which analytics data is to be viewed; either for past week or by specifying dates. Viewing options on the Dashboard include a slider that allows the user to adjust out to one week. The analytics module stores web data history for 90 days before cycling through oldest entries.

The main dashboard gives a thumbnail-style view of the different graphs that are available; a user can double-click on the title bar of each graph to expand that graph for more detail. Within the graphs there is the option to view the data in a visual format or in a table / list format.

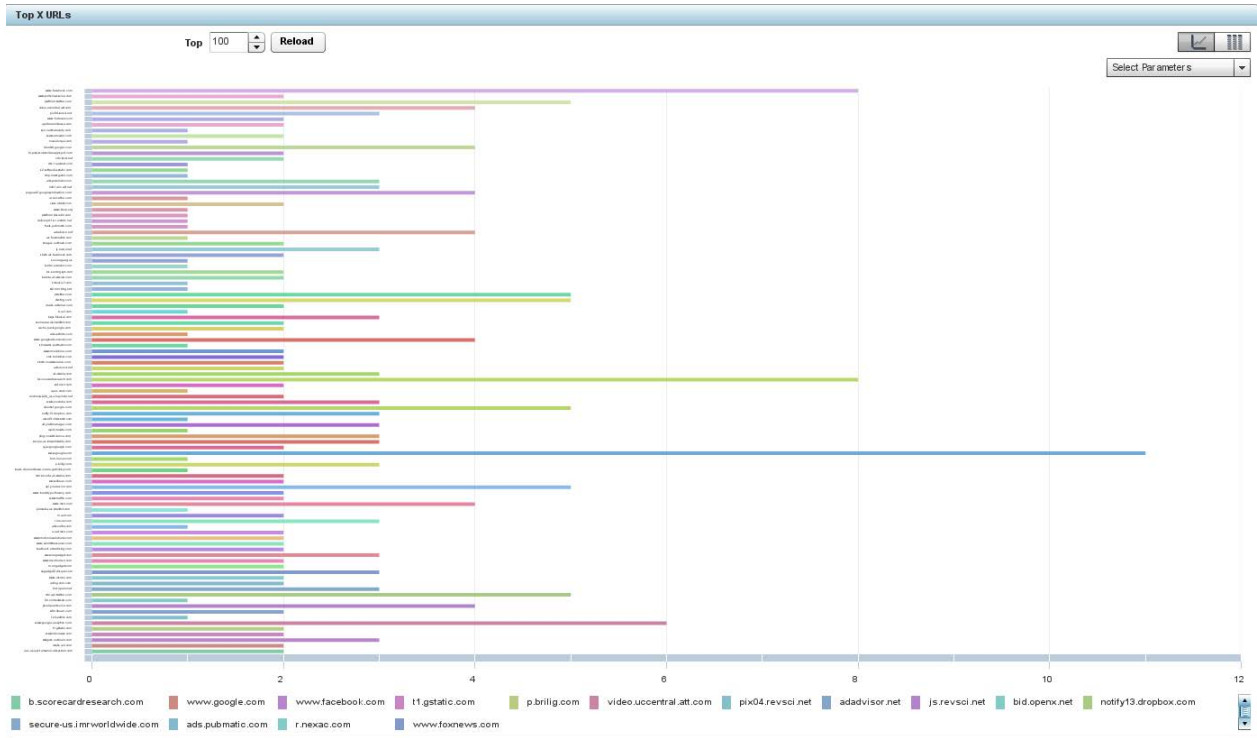


Figure 2 - Top X URLs

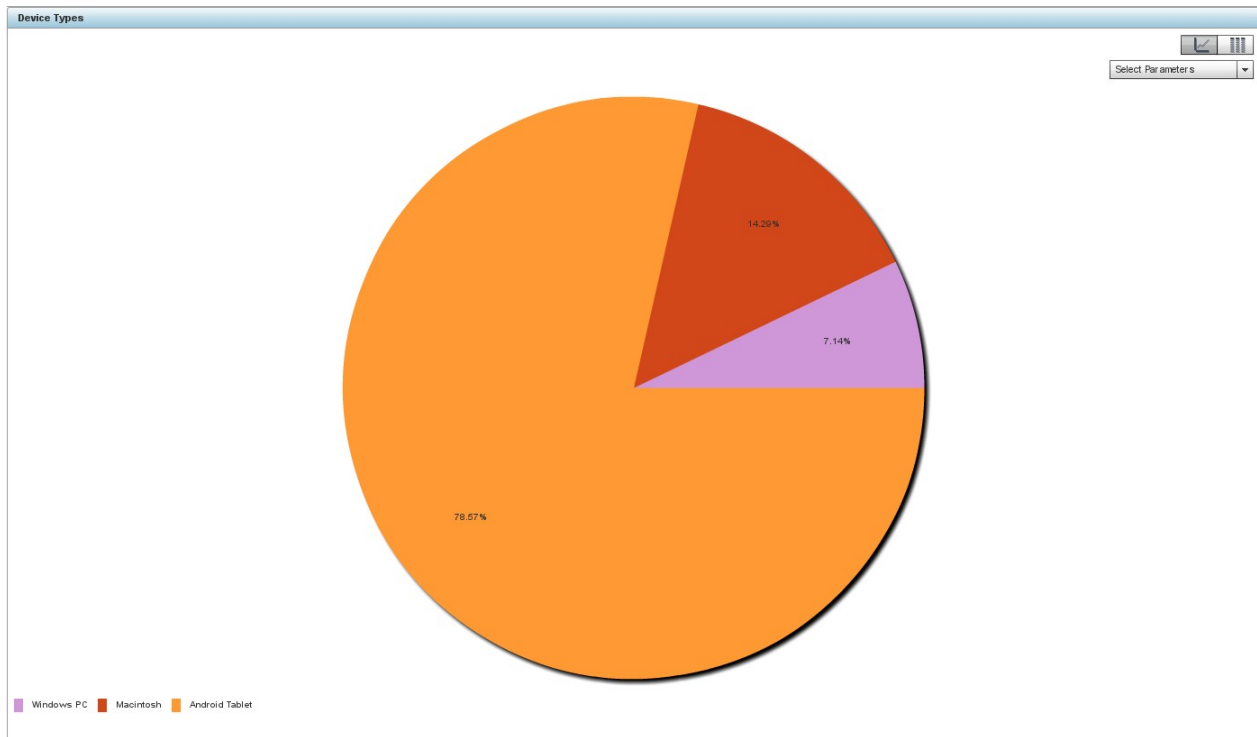


Figure 3 - Device Types

1.3 Components

The Guest Analytics solution is dependent on the following components:

- **Captive Portal** – Though the HTTP Analysis configuration item is available for any WLAN, the Analytics feature, with graphs, etc. is only available on Captive Portal WLAN's. To get any kind of HTTP Analysis on a non-CP WLAN, one would forward traffic to a syslog server and parse from there.
- **WLAN Security / Captive Portal authentication** – used for client access. The Analytics details are pulled by the NX9xxx for Captive Portal WLAN's only.
- **WLAN Security / MAC Registration** – MAC registration facilitates tying a particular device's web traffic with that device as well as providing the device onboarding function after the first association by a client device.
- **WLAN Firewall** – without firewall functionality, we cannot snoop the HTML headers to get the device information. Within the Firewall section of the guest WLAN is where we enable forwarding of HTTP Analytics to the controller.
- **RADIUS** – The MAC authentication will require RADIUS policies to be created

2. Configuration

The following steps are necessary to enable Guest Analytics and are further detailed in the next section:

1. Ensure the NX9xxx platform has an installed license
2. Ensure necessary ports are open through any firewalls in path
3. For MAC registration and authentication, create / map RADIUS policies
4. Create a Captive Portal policy for guest access
5. Create WLAN for guest access
6. Under the Firewall section of your configured WLAN, enable HTTP Analysis forwarding to controller

2.1 Configuration Details

2.1.1 Licensing

Licensing is self-explanatory. Ensure the Analytics license has been purchased and apply it to the NX9xxx controller. This is done within the device context in WiNG 5.x:

Install a License (Device Configuration Context):

```
NX9000(config-device-B4-C7-99-6C-86-5F)# license HTANLT <license-string>
```

View Installed Licenses (Any Context):

```
NX9000# show licenses
```

Serial Number : B4C7996C865F

Device Licenses:

AP-LICENSE

String :


```

Value      : 0
Used       : 0
AAP- LI CENSE
String     : 71e859aa1084dd192f1071b07dc02a9dc34798ac144a2592adf44e107b03e082175b655ccef6768e
Value     : 10240
Used      : 3
ADVANCED- SECURITY
String     : 71e859aa1084dd190c78e2541172408bc34798ac144a259260622a33ba88d7fc078eeae51a66db64
HOTSPOT- ANALYTICS
String     : 3c1c38def86cd97a2af818ffd7b2e097991be267ea3b61284c604e668798df522cd538c7ae18ab03

```

2.1.2 Firewall – Protocols

In some cases the communication between active / standby members of a cluster may happen through a firewall. In order for the related databases to sync correctly, ensure the following ports are open between the cluster members (Active to Standby), to sync the relative tables:

Analytics Database Sync – TCP ports	
<i>Namenode</i>	8020
<i>Datanode</i>	50010
<i>Datanode</i>	50020
<i>Backupnode</i>	50100
<i>Namenode</i>	50070
<i>Datanodes</i>	50075
<i>Secondarynamenode</i>	50090
<i>Backup/Checkpointnode</i>	50105
<i>Master</i>	60000
<i>RegionServer</i>	60020
<i>Zookeeper</i>	2181
<i>Master</i>	60010
<i>RegionServer</i>	60030

2.1.3 RADIUS and AAA Policies

RADIUS services can be provided by an external server or by the on-board RADIUS policies in WiNG.

2.1.3.1 External RADIUS Servers

If using an external server, then only a AAA Policy is needed to point to and establish the parameters for the external server; namely Server Type, as seen below:

Configuration → Wireless → AAA Policy:

Server Id	Host	Port	Server Type	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
1		1,812	onboard-controller	None	3	3s	46	X	X

When configuring an external server, you will need to specify either the hostname or IP address of the server, as selected via the dropdown selector. Enter the shared secret for the external server and select proxy mode, dependent on what WiNG device will be communicating directly with the RADIUS server. Typically for external configurations, either Through Wireless Controller or Through RF-Domain Manager are used.

Authentication Server

Server Id 1

Settings

Host * Hostname ▾

Port ⓘ 1812 (1 to 65,535)

Server Type ✎ Host ▾

Secret * Show

Request Proxy Mode ✎ Through Wireless Controller ▾

Request Attempts ⓘ 3 (1 to 10)

Request Timeout ⓘ 3 Seconds (1 to 60)

Retry Timeout Factor ⓘ 100 (50 to 200)

DSCP ⓘ 46 (0 to 63)

Network Access Identifier Routing

NAI Routing Enable ⓘ

OK Reset Exit

2.1.3.2 On-Board RADIUS and AAA Policies

When the NX9000 is providing RADIUS services, the following policies will need to be created:

- Groups
- User Pools
- Server Policy



Configuration of these policies is beyond the scope of this document and is addressed in various other configuration guides.

Configuration → Services → RADIUS → Groups:

The screenshot shows the WiNG v5.4 configuration interface. The top navigation bar includes Dashboard, Configuration, Diagnostics, Operations, and Statistics. The left sidebar shows a tree view with categories like Captive Portals, DNS Whitelist, DHCP Server Policy, RADIUS, Groups, User Pools, and Server Policy. The main content area is titled 'RADIUS Group' and contains a table with three columns: RADIUS Group Policy, Guest User Group, and Management Group. The first row shows 'mac-reg-group' with red 'X' marks in the Guest User Group and Management Group columns.

RADIUS Group Policy	Guest User Group	Management Group
mac-reg-group	X	X

Alternatively, one can use an external RADIUS server and reflect that within the configured AAA policy.

Configuration → Wireless → AAA Policy:

The screenshot shows the WiNG v5.4 configuration interface. The top navigation bar includes Dashboard, Configuration, Diagnostics, Operations, and Statistics. The left sidebar shows a tree view with categories like Wireless LANs, WLAN QoS Policy, Radio QoS Policy, AAA Policy, Association ACL, SMART RF Policy, MeshConnex Policy, and Mesh QoS Policy. The main content area is titled 'Authentication, Authorization, and Accounting (AAA)' and contains a table with two columns: AAA Policy and Accounting Packet Type. The first row shows 'aaa-htanlt' with 'Start/Stop' in the Accounting Packet Type column.

AAA Policy	Accounting Packet Type
aaa-htanlt	Start/Stop

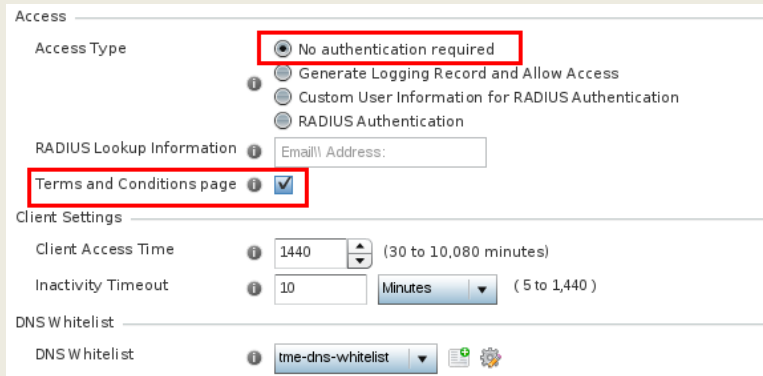
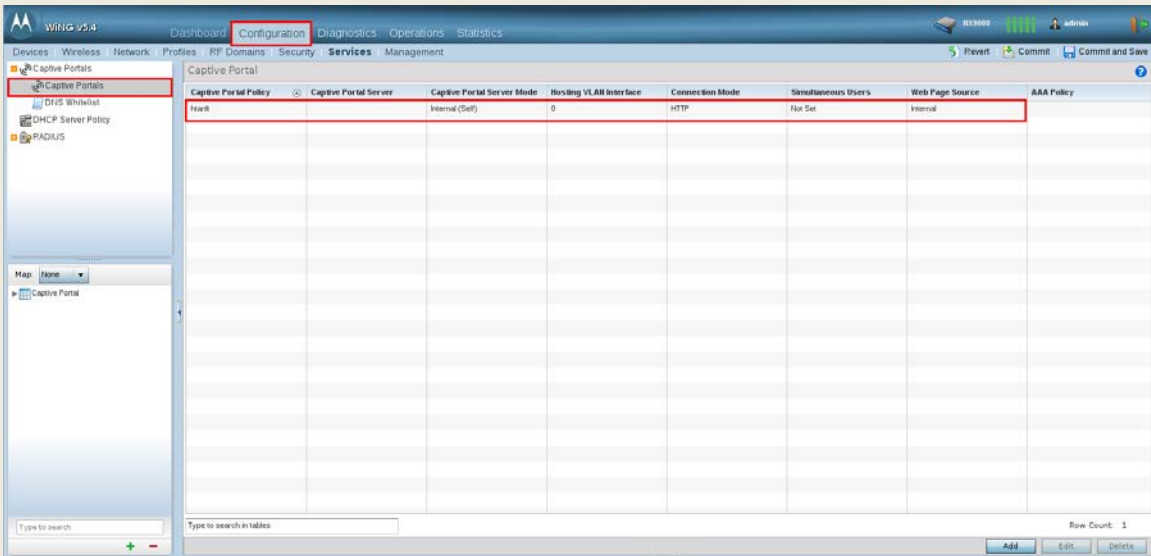
2.1.4 Captive Portal Policies

Captive portal configuration has been covered in previous documents. However the configuration items involved are:

- A WLAN with Captive Portal enabled
- A Captive Portal policy; ensure this policy is applied not only to the WLAN, but also to the device(s) / profile(s) that will host the captive portal pages, if done so on a WiNG device.
 - Customized web pages, either internal to WiNG or externally hosted
 - Access Method – this may be “None”, logging only or perhaps RADIUS. The subsequent elements then are configured also, as necessary.

- Terms and Conditions – aside from the legal reasons to use a T&C page, enabling this can cause the necessary interaction with the user in order to register their mac-address. If “None” or “Generate Logging Record” is selected for Access Method, then Terms and Conditions needs to be enabled to facilitate interaction with the client for mac-registration.
- DNS Whitelist – configure whitelisted DNS servers so that users can initiate a URL call and thus redirection to externally hosted captive portal pages.

Configuration → Services → Captive Portal:



2.1.5 Wireless LAN

Analytics is dependent on four main parameters within the WLAN configuration:

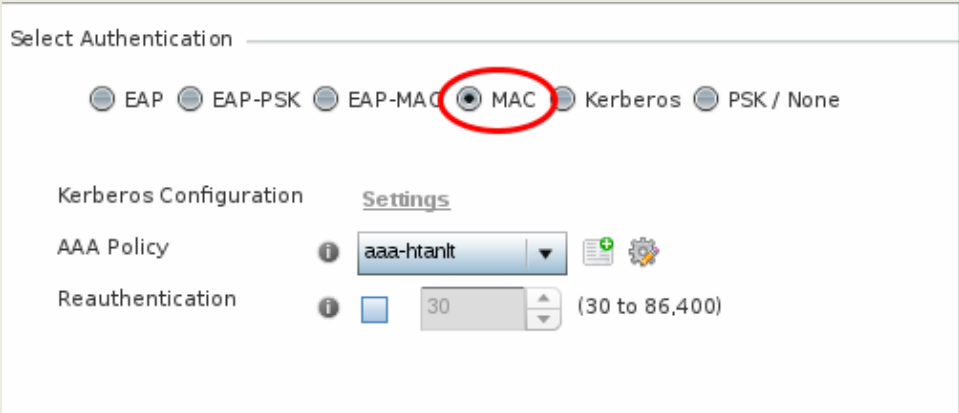
- MAC Authentication
- Captive Portal
- MAC Address registration
- HTTP Analysis under the Firewall section

2.1.5.1 MAC Authentication

MAC authentication will be used in the process of registering the client device mac-addresses. Initially this method will fail, as there will be no entry for the client device. However, after the client is given access via Captive Portal, an entry of the client's mac-address will be made in the MAC database.

As MAC authentication is a RADIUS method, AAA and RADIUS policies will be needed as well:

Configuration → Wireless → Wireless LANs → <WLAN-Name> → Security:



Select Authentication

EAP EAP-PSK EAP-MAC MAC Kerberos PSK / None

Kerberos Configuration [Settings](#)

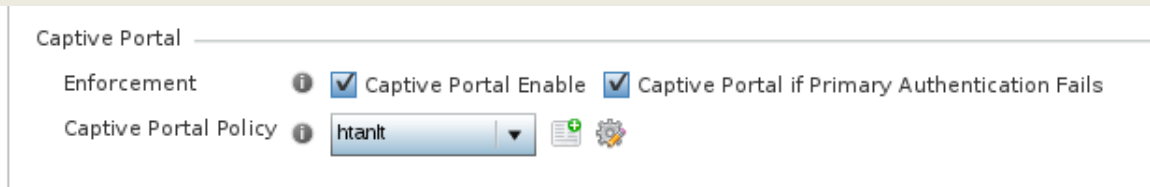
AAA Policy

Reauthentication (30 to 86,400)

2.1.5.2 Captive Portal

As the Analytics features and graphing is only available for Captive Portal traffic, then enforcement must be enabled on your guest WLAN. Additionally, we must provide Captive Portal as a secondary authentication method, because the initial MAC authentication will fail:

Configuration → Wireless → Wireless LANs → <WLAN-Name> → Security:



Captive Portal

Enforcement Captive Portal Enable Captive Portal if Primary Authentication Fails

Captive Portal Policy

After the first time a client connects, they will fail MAC authentication, because there are no entries yet for the client; thus Captive Portal authentication will take place. The subsequent client connections are based on their MAC address entries, which effectively become their “username” / “password” entries for RADIUS authentication.

2.1.5.3 MAC Registration

Enable MAC Registration and specify your RADIUS group to be used:

Configuration → Wireless → Wireless LANs → <WLAN-Name> → Security:

MAC Registration

Enable

Radius Group Name

Expiry Time (1 to 1,500 days)

As stated before, MAC registration is what facilitates the WiNG device learning the identity of the client device and entering it into its database. By default, the expiry period for the learned MAC addresses is 1500 days, meaning that after the initial association by a new client, said client will bypass the captive portal splash page redirect and be automatically authenticated for the next 1500 days or the configured period under **Expiry Time**.

2.1.6 HTTP Analysis

Of course, Zebra's Stateful Packet Inspection firewall is what facilitates snooping of the HTTP headers to obtain the Analytics data. We have three choices here for forwarding of said data:

Forward to Syslog Server – If the user wishes to use syslog and parse with their own tools, this option is available for any WLAN (not just Captive Portal based WLANs)

Forward to Controller – this is the requirement for our own Analytics engine on the NX9xxx platforms. Enable this to forward Captive Portal Traffic to the controller where Analytics is enabled.

Forward to External Analytics Engine – this option enables us to forward to an Nearbuy appliance for their analytics features, if the user has purchased a Nearbuy solution.

HTTP Analysis

Forward To Syslog Server Enable

Host Hostname

Port

Proxy Mode

Forward to Controller Enable

Forward to External Analytics Engine Enable

Filter

Filter Out Images

Strip Query String

Additionally, one may choose to filter images or query strings if that information is not desired or if there is concern over the amount of data stored, etc.

3. Nearby Systems Solution

This section will briefly discuss forwarding to a Nearby solution. It is based on a WiNG 5 hosted Captive Portal, not Nearby.

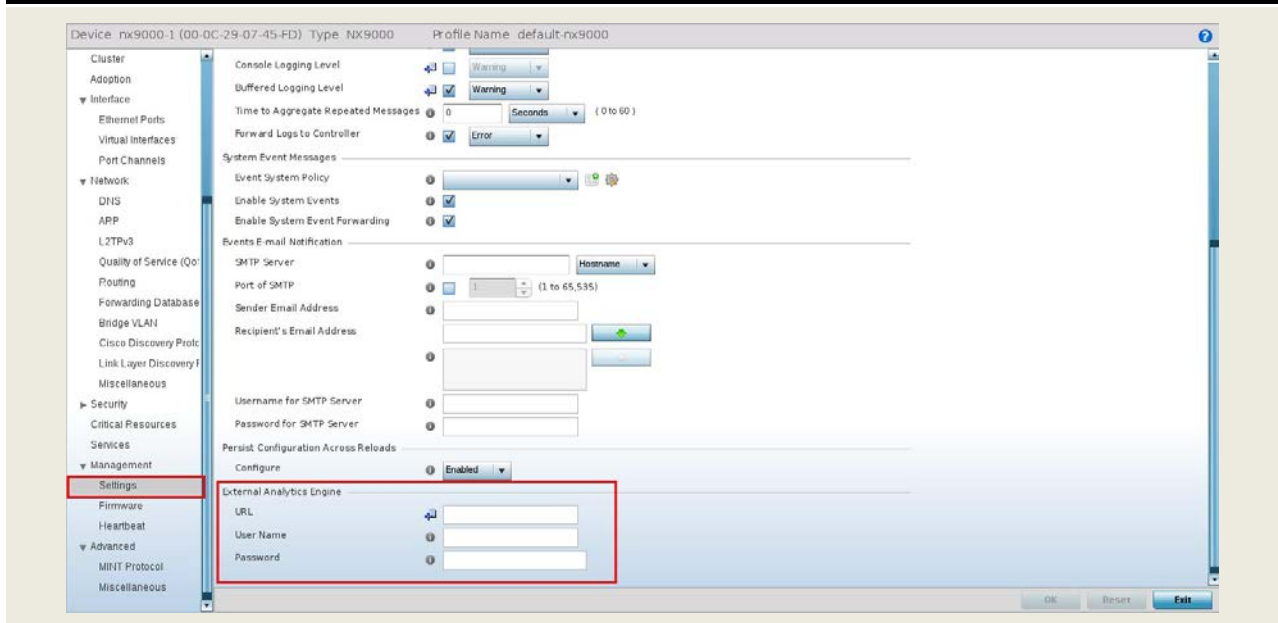
3.1 Nearby External Server Configuration

If we are using a WiNG 5 hosted Captive Portal, yet forwarding analytics data to a Nearby solution, the all of the following, previously listed requisites still apply:

- Analytics license has been applied to NX9xxx platform
- WiNG 5 Guest wifi WLAN is configured
- WiNG 5 Captive Portal is configured
- MAC authentication still applies
- Captive Portal if Primary Fails still applies
- MAC Registration still applies
- RADIUS / AAA Policies are configured

The difference comes in where we are forwarding the captured HTTP analysis traffic. Specify the external device as seen below:

Configuration → Profile → <Profile-Name> → Management → Settings:

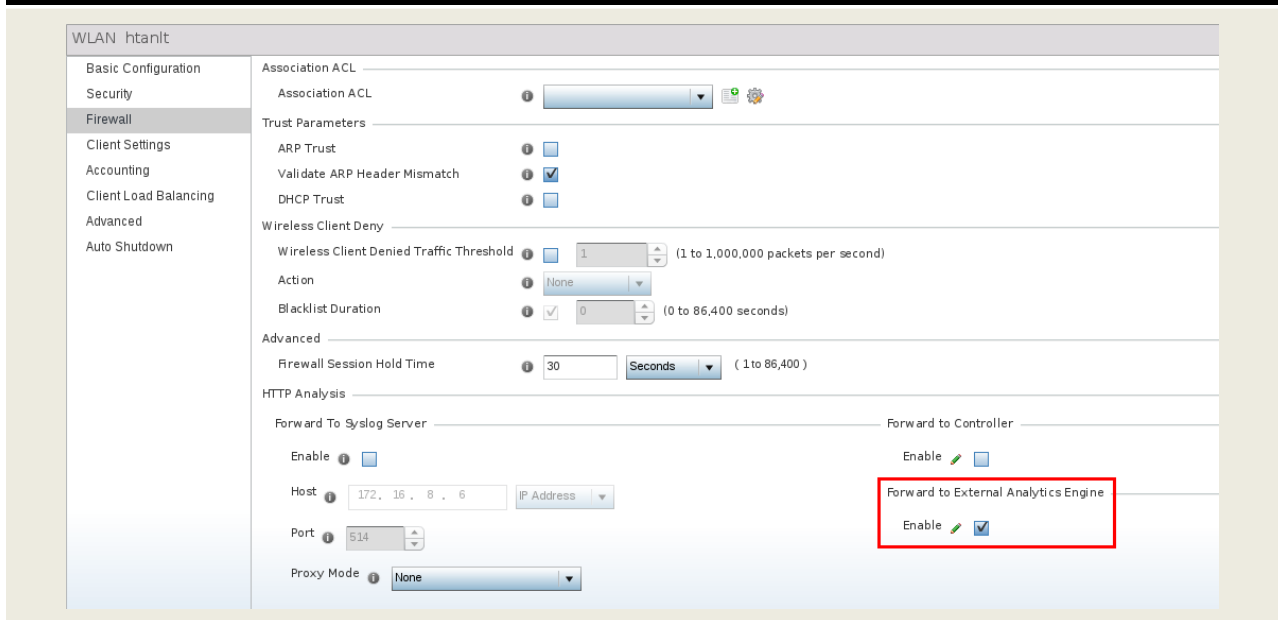


The Nearby solution is a true cloud based Software as a Service (SaaS) product, so it will require the Nearby web URL and account credentials for forwarding to take place.

3.2 HTTP Analysis

In the Wireless LAN enable forwarding to External Analytics Engine:

Configuration → Wireless → Wireless LANs → <WLAN-Name> → Firewall:



4. Appendix

4.1 Running Configuration

```
!  
! Configuration of NX9000 version 5.4.0.0-024D  
!  
!  
version 2.1  
!  
!  
ip access-list BROADCAST-MULTICAST-CONTROL  
  permit tcp any any rule-precedence 10 rule-description "permit all TCP traffic"  
  permit udp any eq 67 any eq dhcp rule-precedence 11 rule-description "permit DHCP replies"  
  deny udp any range 137 138 any range 137 138 rule-precedence 20 rule-description "deny windows netbios"  
  deny ip any 224.0.0.0/4 rule-precedence 21 rule-description "deny IP multicast"  
  deny ip any host 255.255.255.255 rule-precedence 22 rule-description "deny IP local broadcast"  
  permit ip any any rule-precedence 100 rule-description "permit all IP traffic"  
!  
mac access-list PERMIT-ARP-AND-IPv4  
  permit any any type ip rule-precedence 10 rule-description "permit all IPv4 traffic"  
  permit any any type arp rule-precedence 20 rule-description "permit all ARP traffic"  
!  
firewall-policy default  
  no ip dos tcp-sequence-past-window  
  dhcp-offer-convert  
!  
!  
mint-policy global-default  
!  
meshpoint-qos-policy default  
!  
wlan-qos-policy default  
  qos trust dscp  
  qos trust wmm  
!  
radio-qos-policy default  
!  
aaa-policy aaa-htanlt  
  authentication server 1 onboard controller  
!  
dns-whitelist tme-dns-whitelist  
  permit 4.2.2.1  
  permit 172.16.8.6
```

```

!
captive-portal htanlt
  access-type logging
  access-time 30
  custom-auth info Email\\\ Address:
  inactivity-timeout 300
  terms-agreement
  use aaa-policy aaa-htanlt
  use dns-whitelist tme-dns-whitelist
!
wlan htanlt
  ssid htanlt
  vlan 9
  bridging-mode local
  encryption-type none
  authentication-type mac
  use aaa-policy aaa-htanlt
  use captive-portal htanlt
  captive-portal-enforcement fall-back
  mac-registration group-name mac-reg-group expiry-time 1500
  http-analyze controller
!
radius-group mac-reg-group
!
radius-user-pool-policy rad-htanlt-users
!
radius-server-policy rad-htanlt
  use radius-user-pool-policy rad-htanlt-users
!
!
l2tpv3 policy default
!
profile nx9000 default-nx9000
  ip default-gateway 172.16.8.1
  autoinstall configuration
  autoinstall firmware
  no ap-upgrade auto
  use radius-server-policy rad-htanlt
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure

```

```

crypto load-management
interface ge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
interface xge1
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
interface ge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
interface xge2
  ip dhcp trust
  qos trust dscp
  qos trust 802.1p
interface vlan1
  ip address dhcp
  ip address zeroconf secondary
  ip dhcp client request options all
use firewall-policy default
logging on
service pm sys-restart
!
profile ap71xx default-ap71xx
  autoinstall configuration
  autoinstall firmware
  crypto ikev1 policy ikev1-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ikev2 policy ikev2-default
    isakmp-proposal default encryption aes-256 group 2 hash sha
  crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
  crypto ikev1 remote-vpn
  crypto ikev2 remote-vpn
  crypto auto-ipsec-secure
interface radio1
  shutdown
interface radio2
  channel 140
  power 7
  wlan htanlt bss 1 primary
interface radio3
interface ge1
  switchport mode trunk
  switchport trunk native vlan 9

```

```

no switchport trunk native tagged
switchport trunk allowed vlan 9-11
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface ge2
ip dhcp trust
qos trust dscp
qos trust 802.1p
interface vlan1
shutdown
interface vlan9
ip address dhcp
ip dhcp client request options all
interface wwan1
interface pppoe1
use firewall-policy default
use captive-portal server htanlt
logging on
service pm sys-restart
router ospf
!
!
rf-domain default
country-code us
!
rf-domain store-1
timezone Etc/GMT-7
country-code us
!
nx9000 00-0C-29-07-45-FD
use profile default-nx9000
use rf-domain default
hostname nx9000-1
license AAP 185f5fa6b3bda9b3d4f22018f87ccb3076fcfbb2023aeb7be24c93b471de2227cbc497109222a46f
license HTANLT 185f5fa6b3bda9b36f34944e2764de4e76fcfbb2023aeb7bb596f423ca7ab5c0915967eddc13e2c6
timezone Etc/GMT-7
no mint mlcp vlan
ip default-gateway 172.16.8.1
use radius-server-policy rad-htanlt
interface vlan1
ip address 172.16.8.10/24
logging on
no logging console
logging buffered warnings
!

```

```
ap71xx 00-23-68-93-13-CC
  use profile default-ap71xx
  use rf-domain store-1
  hostname ap7131-9313CC
!
ap71xx 00-23-68-9E-51-44
  use profile default-ap71xx
  use rf-domain store-1
  hostname ap7131-9E5144
!
!
end
```

